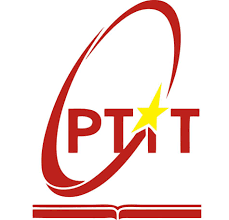


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIÊN THÔNG

**KHOA CÔNG NGHỆ THÔNG TIN**

**----------**



**BÁO CÁO MÔN HỌC**

**HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX**

**Nhóm 03**

**Giảng viên: Phạm Hoàng Duy**

**Nhóm báo cáo: Nhóm báo cáo 10**

**Các thành viên trong nhóm:**

**Nguyễn Thế Thăng Long – B16DCAT097**

**Hoàng Ngọc Thuần – B16DCAT163**

**Trần Văn Khải – B16DCAT081**

**Nguyễn Quang Hưng – B16DCAT074**

Hà nội, 2019

Mục lục

[1](#_Toc7557542)

[Câu 1: Dịch vụ DNS/DHCP (Nguyễn Thế Thăng Long ) 3](#_Toc7557543)

[1. Dịch vụ DNS/DHCP trên máy chủ Windows Sever 3](#_Toc7557544)

[a) Dịch vụ DNS 3](#_Toc7557545)

[b) Dịch vụ DHCP 3](#_Toc7557546)

[2. Dịch vụ DNS/DHCP trên máy chủ Linux/ Unix Sever 4](#_Toc7557547)

[a) Dịch vụ DNS 4](#_Toc7557548)

[b) Dịch vụ DHCP 5](#_Toc7557549)

[Câu 2: Tìm hiểu về dịch vụ chia sẻ File và máy in (Hoàng Ngọc Thuần) 6](#_Toc7557550)

[Dịch vụ file trong Windows 6](#_Toc7557551)

[Dịch vụ file trong Linux 7](#_Toc7557552)

[Dịch vụ file FTP 7](#_Toc7557553)

[Dịch vụ file NFS 8](#_Toc7557554)

[Chia sẻ file và máy in giữa các máy Linux với Window 9](#_Toc7557555)

[Dịch vụ chia sẻ máy in trong windows 10](#_Toc7557556)

[Dịch vụ chia sẻ máy in trong Linux 10](#_Toc7557557)

[Câu 4: Cài đặt và quản lý trang Web (Trần Văn Khải ) 11](#_Toc7557558)

[Điểm chung giữa 2 hệ điều hành: 11](#_Toc7557559)

[Cài đặt: 11](#_Toc7557560)

[**1.** **Windows** 11](#_Toc7557561)

[**2.** **Ubuntu(Linux)** 13](#_Toc7557562)

[Quản trị 14](#_Toc7557563)

[1. **Windows** 14](#_Toc7557564)

[2. **Ubuntu(Linux)** 15](#_Toc7557565)

[Câu 5: Truy cập từ xa (Nguyễn Quang Hưng) 15](#_Toc7557566)

[**1. Cài đặt** 15](#_Toc7557567)

[**a. Windows server 2008** 15](#_Toc7557568)

[**b) Ubuntu server** 17](#_Toc7557569)

[**2. Quản trị** 18](#_Toc7557570)

[**a) Windows Server 2008** 18](#_Toc7557571)

[**b) Ubuntu server** 19](#_Toc7557572)

# Câu 1: Dịch vụ DNS/DHCP (Nguyễn Thế Thăng Long )

## 1. Dịch vụ DNS/DHCP trên máy chủ Windows Sever

### a) Dịch vụ DNS

Dịch vụ tên miền DNS ( Domain Name Service): là hệ thống quản lý cơ sở dữ liệu phân tán dựa trên mồ hình phân cấp chủ/khách để chuyển đổi tên máy chủ / tên miền thành địa chỉ IP. Khi người dùng truy cập tài nguyên mạng, dịch vụ DNS trên máy tính sẽ xác định vị trí vật lí của máy tính tính chứa nội dung muốn truy cập

**Ưu điểm của DNS:**

* Đơn giản và dễ sử dụng: Người dùng chỉ cần nhớ tên của máy tính hay tài nguyên mạng
* Mở rộng: Phân tán công việc phân rã tên/ địa chỉ mạng trên nhiều máy chủ và cơ sở dữ liệu
* Tính nhất quản: Các địa chỉ mạng có thể thay đổi trong khi tên của máy vẫn giữ nguyên làm cho các tài nguyên mạng dễ xác định hơn

**Cài đặt DNS:**

* Cài đặt thông qua tiện ích “Sever Manager”
* Máy chủ DNS có thể quản lý miền chính (pimary zone) hoặc miền thứ cấp (secondary zone) hoặc cả hai. Miền chính cho phép cập nhật bản ghi về tên miền, trong khi đó miền thứ cấp không cho phép sửa đổi các bản ghi tên miền mà chỉ lưu bản sao của miền chính. Khi đặt cấu hình cho máy chủ DNS có 2 kiểu vùng khác nhau:
  + Vùng tìm kiếm thuận (Forward Lookup Zone): cho phép máy tính truy vấn địa chỉ Internet ứng với một tên
  + Vùng tìm kiếm nghịch (Reverse Lookup Zone): là việc ngược lại trả lại tên miền ứng với địa chỉ Internet

**Một số vấn đề khi cài đặt DNS:**

* Số các mạng vật lý cần dịch vụ DNS
* Số lượng máy chủ DNS
* Băng thông WAN Số miền hay vùng
* Các dạng và số lượng bản ghi

### b) Dịch vụ DHCP

Dịch vụ DHCP (Dynamic Host Configuration Protocol) giúp quản lý và cấp phát tập trung và tự động địa chỉ mạng Internet cho các máy tính trong mạng. Máy chủ DHCP duy trì danh sách các địa chỉ IP và cấp cho các máy tính trong mạng sử dụng theo khoảng thời gian xác định. Sử dụng DHCP làm cho việc cấu hình mạng trở nên dễ dàng đặc biệt khi có nhiều máy tính

Với việc cấp phát động, người quản trị cần xác định dải địa chỉ cần cấp phát, dải địa chỉ dành riêng/ dự phòng, và khoảng thời gian “sống’ của địa chỉ được cấp phát. Có thể cài đặt máy chủ DHCP qua tiện ích “Sever Manager”

**Một số vấn đề khi cài đặt DHCP:**

* Số lượng mạng vật lý hay lo-gic cần tự động cấu hình IP
* Vị trí bộ định tuyến
* Số mạng LAN ảo

**Các câu lệnh kiểm tra:**

* ping: kiểm tra kết nối mạng đến một máy tính trong Internet
* nslookup: kiểm tra việc cài đặt cấu hình DNS
* ipconfig: xem các tham số mạng được đặt cho máy tính như địa chỉ mạng, địa chỉ máy chủ DNS.

## 2. Dịch vụ DNS/DHCP trên máy chủ Linux/ Unix Sever

### a) Dịch vụ DNS

Dịch vụ DNS là dịch vụ tên miền Internet mà tạo ánh xạ từ địa chỉ Internet ra tên miền đầy đủ và ngược lại. Máy chủ cung cấp dịch vụ DNS chia ra 3 loại :

* Máy chủ chính (primary sever): lưu cơ sở dữ liệu về tên/ địa chỉ Internet cho một vùng và chịu trách nhiệm trả lời truy vấn cho vùng đó
* Máy chủ phụ (secondary server): đóng vai trò ứng cứu và chia sẻ tải cho máy chủ chính. Máy chủ phụ lấy dữ liệu từ máy chủ chính trong vùng đó và trả lời các truy vấn bên trong một miền
* Đệm (caching server): lưu bản sao các truy vấn/kết quả. Máy chủ này không chứa các file cấu hình cho miền cụ thể nào

**Cài đặt DNS** qua gói phần mềm BIND bằng lệnh: “sudo apt-get-install bind9”. Để cài đặt máy chủ tên miền chính cho miền “example.com”, người quản trị cần sửa đổi file cấu hình /etc/bind/etc/bind/named.conf.local

Tạo dữ liệu cho file db.example.com chứa các dữ liệu về tên miền và địa chỉ Internet bằng cách xây dựng các bản ghi

* Bản ghi SOA: bản ghi khởi đầu cho các mục khác trong file và mô tả các tham số cấu hình cơbbản như số sê-ri của dữ liệu, tên miền gốc, thời gian làm mới, thời gian đệm …
* Bản ghi NS: thông báo máy chủ lưu các bản ghi cho vùng tên miền theo cấu trúc “ns IN A địa\_chỉ\_IP”.   
  Ví dụ: ns IN A 192.168.1.10
* Bản ghi A: cho biết tên và địa chỉ Internet theo cấu trúc   
  “Tên IN A địa\_chỉ\_IP”. Ví dụ: www IN A 192.168.1.12
* Bản ghi CNAME: tạo ánh xạ tới bản ghi A,   
  ví dụ: Web IN CNAME www
* Bản ghi PTR: tạo ánh xạ từ địa chỉ sang tên theo cấu trúc “Địa\_chỉ\_IP IN PTR tên\_đầy đủ”.   
  Ví dụ: 192.168.1.2 IN PTR mail.mydomain

**Các câu lệnh kiểm tra**

* Ping: kiểm tra máy trạm gắn với tên miền hoạt động hay không
* Named-checkzone: kiểm tra dữ liệu tên Named-checkzone

### b) Dịch vụ DHCP

Dịch vụ DHCP là dịch vụ mạng cho phép gán cấu hình mạng tự động động cho các máy tính trong mạng

**Thông tin cấu hình mạng gồm có:**

* Địa chỉ internet và mạng con
* Địa chỉ internet của máy cổng
* Địa chỉ internet của máy chủ tên miền

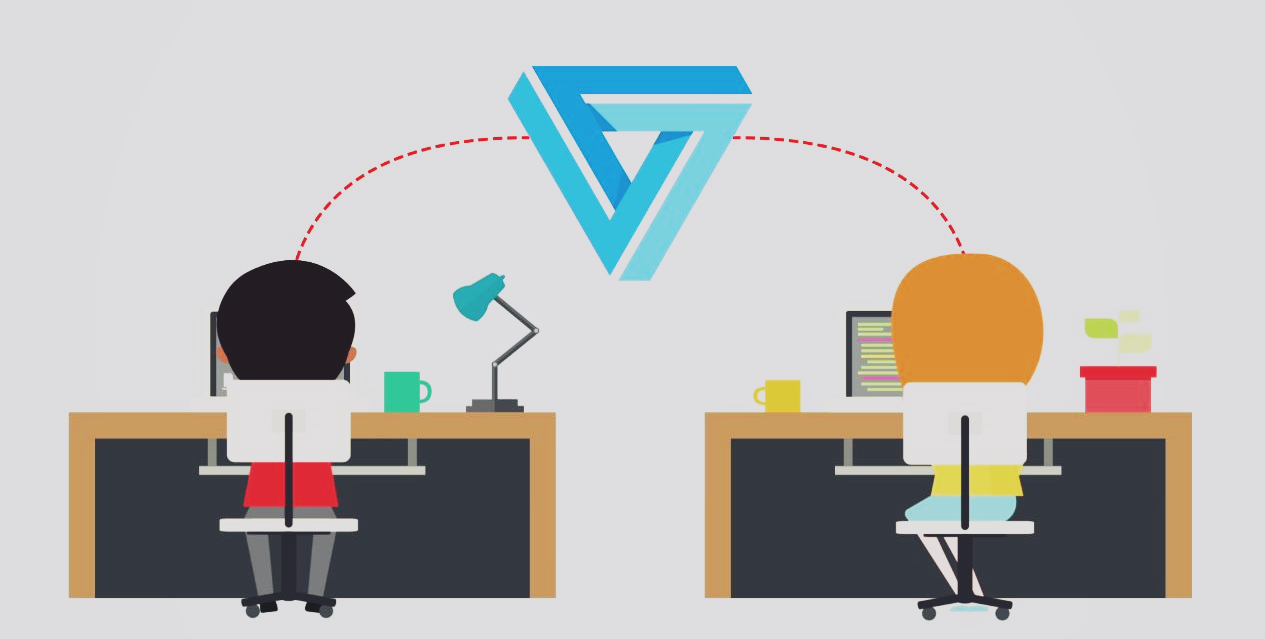
**Các chế độ hoạt động của máy chủ DHCP:**

* Cấp phát tĩnh: Gán thông tin cấu hình mạng không đổi cho máy trạm căn cứ vào địa chỉ vật lý của kết nối mạng mỗi khi có yêu cầu từ máy trạm.
* Cấp phát động: Gán thông tin cấu hình mạng từ dải địa chỉ định trước trong một khoảng thười gian nhất định còn gọi là thời gian mượn địa chỉ. Khi hết hạn cấu hình này có thể được gán cho máy khác.
* Cấp phát tự động: Tự động gán cấu hình mạng cố định từ dải địa chỉ định trước cho thiết bị yêu cầu. So với phương pháp cấp phát động, thông tin cấu hình mạng không bị hết hạn.

Để cài đặt DHCP server sử dụng câu lệnh sau: “sudo apt-get install isc-dhcp-server”. Các thông tin cài đặt cho máy chủ DHCP được lưu tại /etc/default/isc-dhcp-server. Thông tin về địa chỉ cấp cho các máy tính trong mạng được mô tả trong file /etc/dhcp/dhcpd.conf.

Người quản trị kiểm tra các yêu cầu cấp phát được bằng cách kiểm tra nội dung file nhật ký /var/lib/dhcpd.leases hay trạng thái của dịch vụ service isc-dhcp-server status

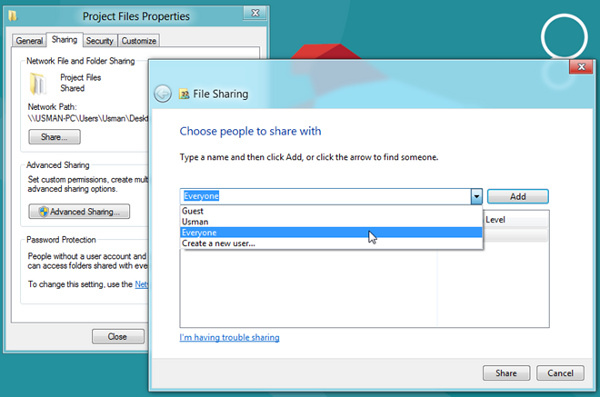
# Câu 2: Tìm hiểu về dịch vụ chia sẻ File và máy in (Hoàng Ngọc Thuần)

 **Giới thiệu về dịch vụ file và dịch vụ in ấn**

- Dịch vụ file cho phép người dùng lưu trữ và chia sẻ các dữ liệu, chương trình với người dùng khác trong mạng.

- Dịch vụ in cho phép các máy in mạng được kết nối trực tiếp với mạng hay thông qua máy tính cho phép người dùng trong mạng có thể sử dụng các dịch vụ của máy in. Các máy chủ in ấn là máy tính kết nối với máy in và làm nhiệm vụ xử lý các yêu cầu in ấn từ các người dùng trong mạng.

## Dịch vụ file trong Windows

****

Trong môi trường Windows có thể áp dụng hai hình thức đảm bảo an ninh đối với việc truy nhập thành công các file chia sẻ căn cứ vào quyền truy nhập của người dùng.

- Quyền với thư mục chia sẻ. Hình thức này chỉ áp dụng với thư mục và các quyền của người dùng giới hạn: Đọc/Ghi/Sở hữu

- Đặt quyền file/thư mục sử dụng cách thức phân quyền NTFS để kiểm soát việc truy nhập. Hình thức này cho phép giám sát tốt hơn và các quyền chi tiết hơn.

Việc thực hiện chia sẻ file có thể được thực hiện trực tiếp từ trình duyệt file của Windows.

- Việc quản lý file được thực hiện thông qua tiện ích *File Server Resource Manager*.

## Dịch vụ file trong Linux

Trong Linux có hai dịch vụ file cơ bản là

- Dịch vụ truyền file qua FTP

- Dịch vụ file mạng NFS

## Description: https://lh3.googleusercontent.com/Wum4FmFC5sYVpHfCQaCPdfftSZkNxKaul5way1Ns1zmjW_8Paqk-HAyxcXi7FTFblAWBW_2Pjl6VrzaCw4yjlqFehshRwXBXnqdz9jinshkJ4DjZOrUhew_1FHSyiJd2frgI2moNDịch vụ file FTP

- Sử dụng để trao đổi các file dùng chung

- Hoạt động theo cơ chế client/server và dùng hai cổng là 21 để điều khiển và cổng 20 để trao đổi dữ liệu

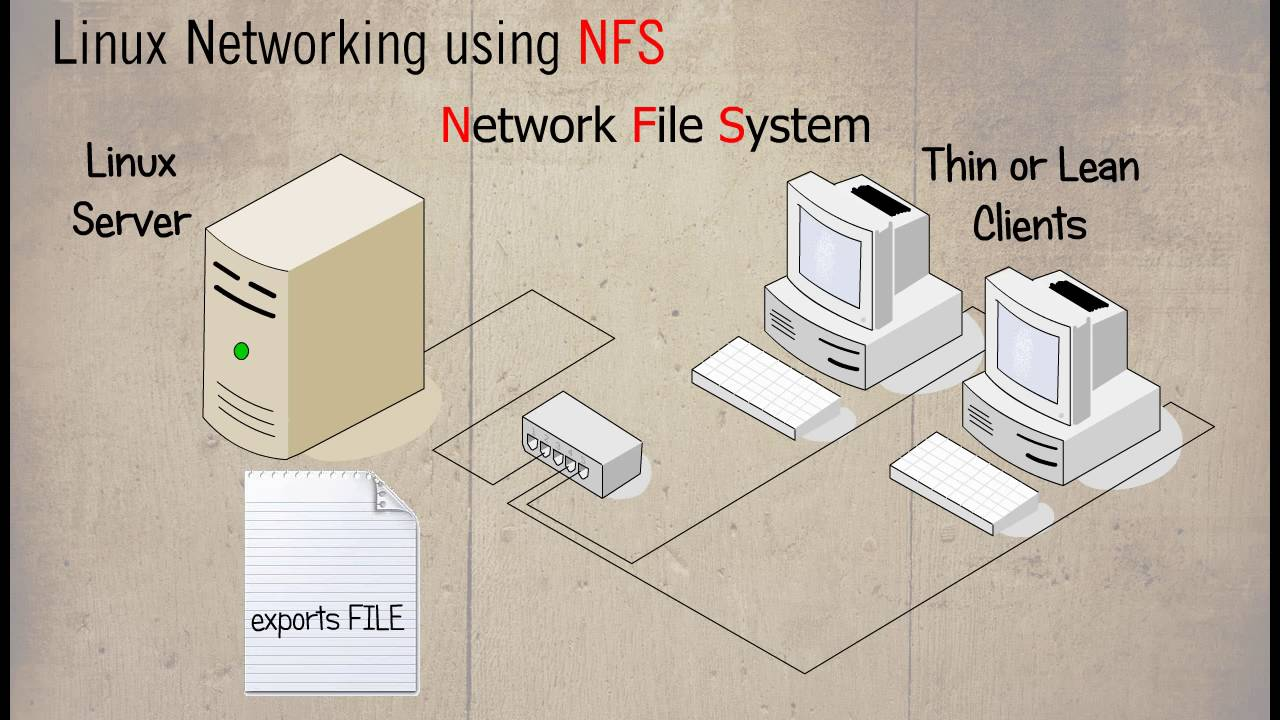
Cài đặt dịch vụ trên Ubuntu:

Các thư mục chia sẻ file được mặc định tại */svr/ftp*

Các thông tin cấu hình: */etc/vsftpd.conf*

Người dùng cần cài chương trình khách FTP để sử dụng dịch vụ

## Dịch vụ file NFS

****

Cho phép người dùng sử dụng file/thư mục trên máy tính mạng giống như trong ổ đĩa cục bộ. Dịch vụ NFS hoạt động theo mô hình chủ/khách.

* Máy chủ chia sẻ thư mục /shared
* Máy khách truy nhập vào thư mục chia sẻ trên máy chủ server:/shared qua câu lệnh mount

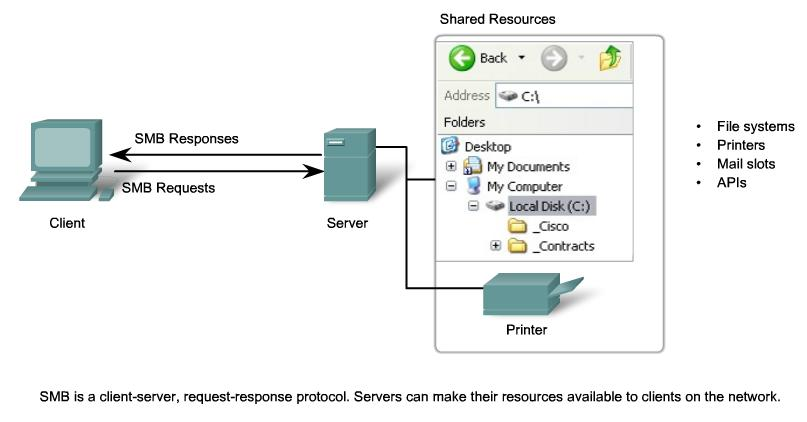
Ưu điểm của dịch vụ NFS là cho phép tiết kiệm không gian lưu trữ trên các máy trạm nhờ vào việc cất giữ các dữ liệu dùng chung lên máy chủ mà truy cập được qua mạng. Người dùng không cần phải có thư mục gốc (home) riêng biệt trên các máy trạm. Câu lệnh dưới đây cài đặt dịch vụ NFS:

*sudo apt-get install nfs-kernel-server*

Để khởi động, dừng hay kiểm tra trạng thái dịch vụ người quản trị có thể dùng câu lệnh

*sudo service nfs-kernel-server start/restart/stop/status*

## Chia sẻ file và máy in giữa các máy Linux với Window

****

- Chạy trên nền giao thức SMB (Server Message Block). SMB là giao thức được các hệ điều hành của Microsoft sử dụng để chia sẻ dữ liệu qua mạng. Linux Samba cũng dựa vào giao thức SMB để viết ra một số tiến trình điển hình như smbd, nmbd, để “nói chuyện “ với các hệ điều hành của Microsoft để người dùng có thể làm việc với máy Linux qua Network Neighborhood.

- Cài đặt trên Ubuntu:

*sudo apt-get update*

*sudo apt-get install samba*

File cấu hình: *smb.conf*

Để truy cập vào mạng chia sẻ

*sudo apt-get install smbclient*

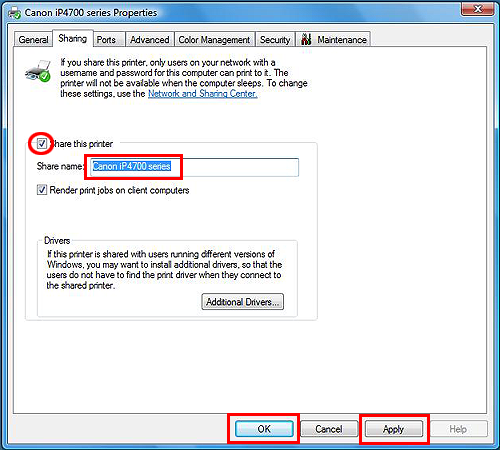
     # List all shares:

*smbclient -L //<HOST\_IP\_OR\_NAME>/<folder\_name> -U <user>*

     # connect:

*smbclient //<HOST\_IP\_OR\_NAME>/<folder\_name> -U <user>*

## Dịch vụ chia sẻ máy in trong windows

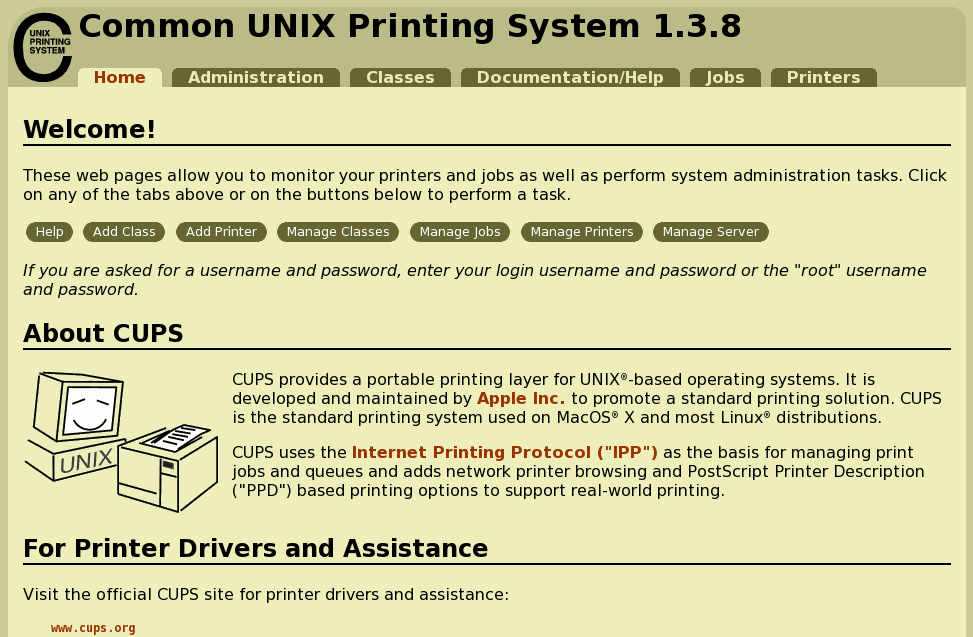
****

Windows phân biệt:

* Thiết bị in (máy in vật lý): kết nối trực tiếp với máy chủ
* Máy in (máy in lô-gíc): giao tiếp với máy in vật lý
* Trình điều khiển máy in: giúp giao tiếp với máy in và che dấu thông tin chi tiết về máy in.

Để máy tính kết nối được với máy in cần có trình điều khiển thích hợp và để chia sẻ máy in vật lý cần cài đặt máy in phù hợp. Việc chia sẻ máy in có thể được thực hiện dễ dàng thông qua giao diện của Windows sau khi cài đặt thành công trình điều khiển.

## Dịch vụ chia sẻ máy in trong Linux

****

- Dịch vụ CUPS (Common UNIX Printing System) cung cấp dịch vụ in ấn và quản lý in cho người dùng sử dụng giao thức chuẩn in ấn Internet (Internet Printing Protocol).

tự động phát hiện các máy in mạng và cung cấp các công cụ quản trị và đặt cấu hình đơn giản qua Web.  
- CUPS được cài qua gói quản lý phần mềm nhờ câu lệnh sudo apt-get install cups.

- Các thông tin cấu hình CUPS được lưu trong file */etc/cups/cupsd.conf*. Các cấu hình cơ bản gồm có:  
Địa chỉ quản trị: *ServerAdmin địa\_chỉ\_email\_quản\_trị*Cổng hoạt động: *Listen 192.168.1.2:631*  
Cho phép sử dụng dịch vụ: *Allow from 192.168.0.\**  
Từ chối dịch vụ : *Deny from all*

Ngoài ra người quản trị có thể cấu hình thông qua giao diện Web tại địa chỉ ngầm định  
*http://localhost:631/admin*.  
Phía máy khách sử dụng câu lệnh lpr để in các file tài liệu cần thiết theo dạng : lpr file\_cần\_in.  
Trong quá trình hoạt động, CUPS ghi nhật ký hoạt động vào thư mục */var/log/cups*.

# Câu 4: Cài đặt và quản lý trang Web (Trần Văn Khải )

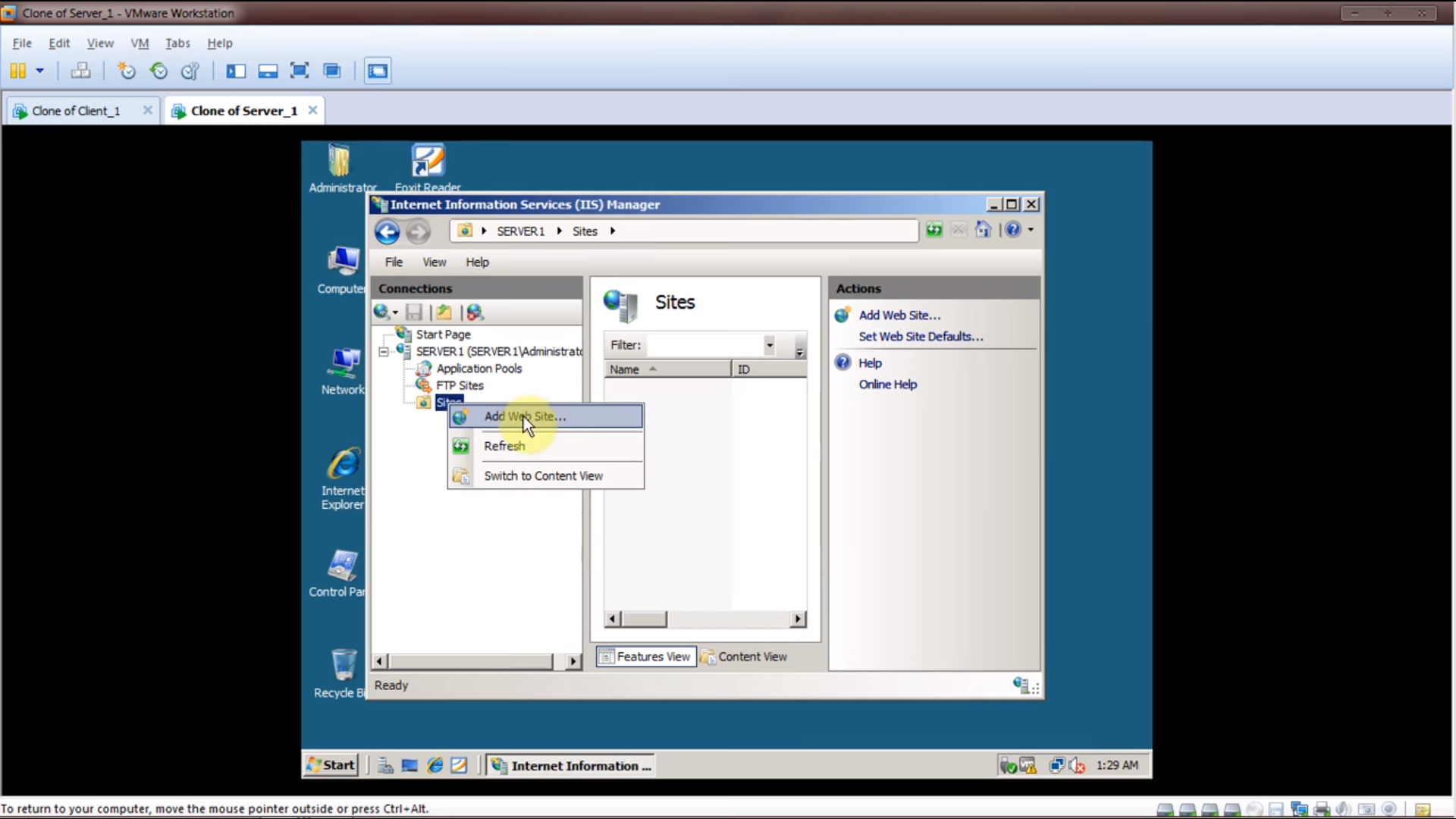
## Điểm chung giữa 2 hệ điều hành:

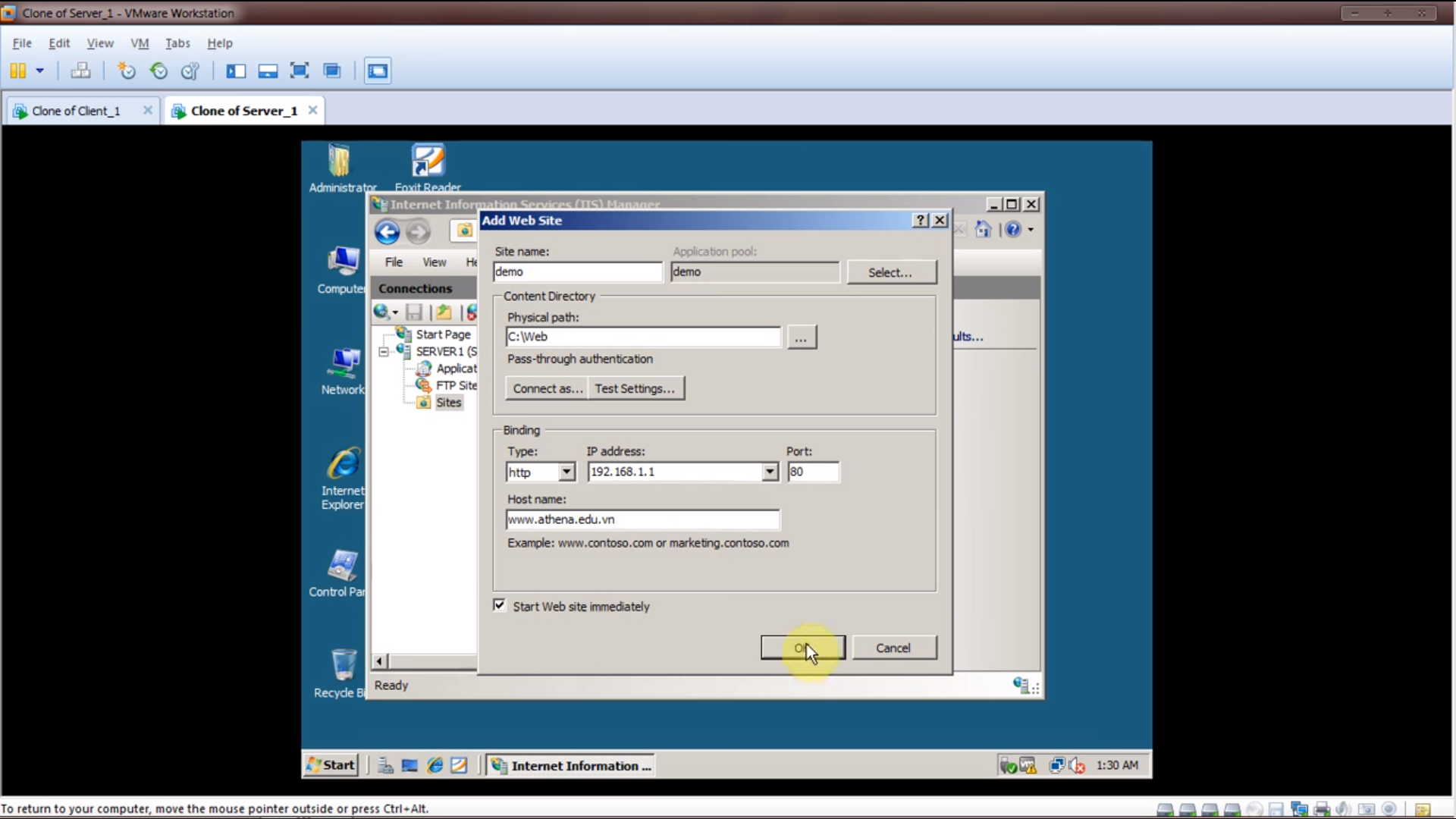
* Cả 2 hệ điều hành đều sử dụng chung cổng 80.

## Cài đặt:

1. **Windows**

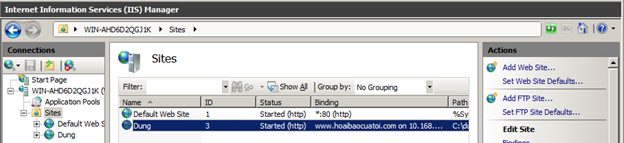
* Trang web trong windows là hệ thống các tài liệu ở dạng siêu văn bản liên kết với nhau(Trang web) mà người dùng có thể xem bằng trình duyệt. Các tài liệu web được soạn thào bằng ngôn ngữ đánh dấu HTML. Các trang web được lưu trong máy chủ web và dùng cổng 80 để truy cập vào.
* Máy chủ: Web server – Information internet Services(IIS)
* Tính năng:
* Giao diện thân thiện, mã nguồn đóng.
* File cấu trúc thư mục ngầm định: Mystie/index.htm
* Đa dạng nhiều tính năng như có thể gửi thư điện tử thông qua dịch vụ thông tin này.
* Cài đặt:

Trong hộp thoại **Internet Information Service(IIS) Manager** mở **SERVER 1** chọn **site** và chọn **add web site…**

Ta cài đặt các thông số cho website: 

* Application pool: xác định các ứng dụng được sử dụng trong trang web.
* Physical path: nơi lưu trữ các file dữ liệu cho trang chủ.
* Host name: là địa chỉ của trang web.

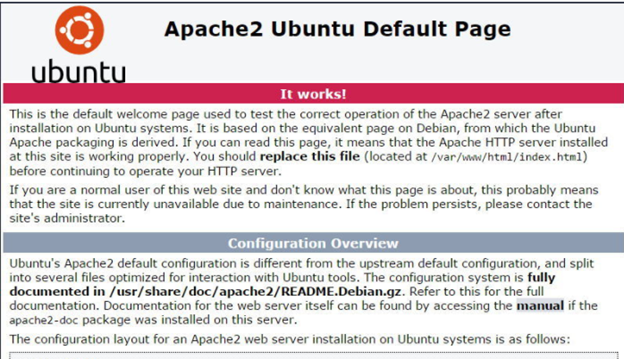
Chỉ cần những thông số cơ bản là ta có thể tạo được một trang web.



1. **Ubuntu(Linux)**

* Máy chủ web là phần mềm chịu trách nghiệm tiếp nhận các truy vấn dưới chuẩn giao thức truyền siêu van bản từ máy khách, rồi gửi trả kết quả xử lý dưới dạng các tài liệu theo chuản HTML
* Linux: Web Server – Apache2
* Tính năng:
* Linh hoạt và dễ cấu hình
* Hỗ trợ xác thực để hạn chế truy cập từ người dùng
* Sự dụng các câu lệnh và mà nguồn mở.
* Cài đặt

Gõ lệnh: sudo apt – get install apache2



Nội dung file cấu hình.



Sau khi cài đặt thành công file cấu hình, người quản trị thực hiện các

câu lệnh như sau đây để các thay đổi có hiệu lực:

*sudo a2ensite mynewsite*

*sudo service apache2 restart*

Khi muốn loại bỏ địa chỉ trang Web hiện có, người quản trị thực hiện

các câu lệnh sau (mynewsite là tên gán với địa chỉ trang Web)

*sudo a2ensite mynewsite*

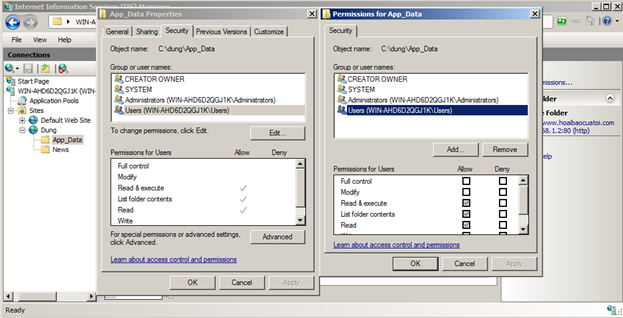
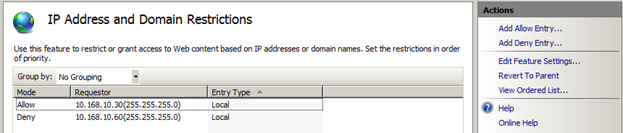
*sudo service apache2 restart*

## Quản trị

Hai môi trường đều cho phep quản trị viên kiểm soát cá truy cập tới trang web và thay đổi cài đặt, kiểm soát tài nguyên…

1. **Windows**

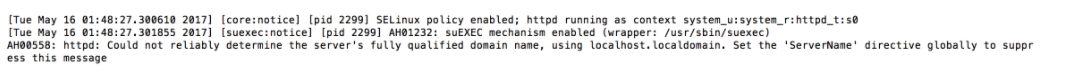
* Hạn chế về địa chỉ mạng thông quan chức năng thiết lập luật hạn chế **(Add Allow Restriction Rule**) của máy chủ IIS



1. **Ubuntu(Linux)**

* Các bản ghi và các file cấu hình , nhật ký các cấp cảnh báo của máy chủ web
* **access.log**: toàn bộ các lần thử truy nhập vào máy chủ, liệt kê địa chỉ của máy khách, thời gian, yêu cầu cụ thể và thông tin về trình duyệt được sử dụng.



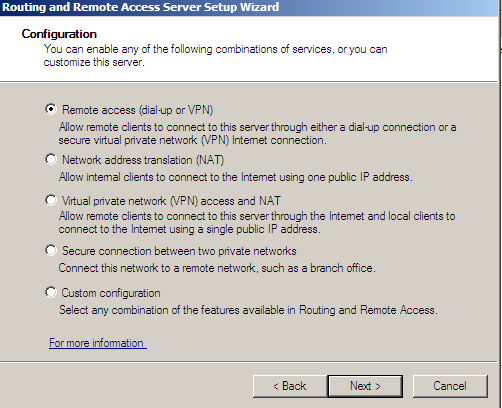
* **error.log**: biết toàn bộ các lỗi và mức độ cảnh báo mà dịch vụ Web gặp phải khi xử lý các yêu cầu truy nhập, các trang không tìm thấy, các thư mục bị từ chối truy nhập. 

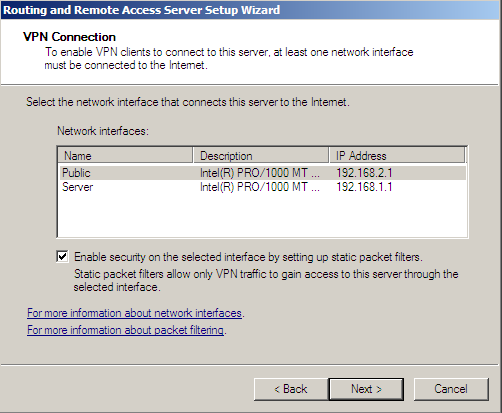
# Câu 5: Truy cập từ xa (Nguyễn Quang Hưng)

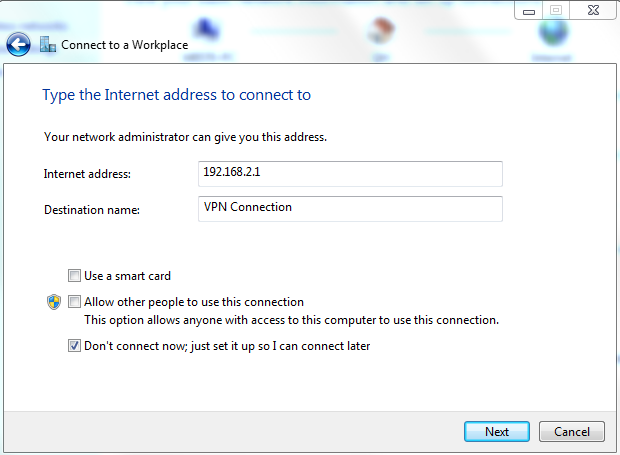
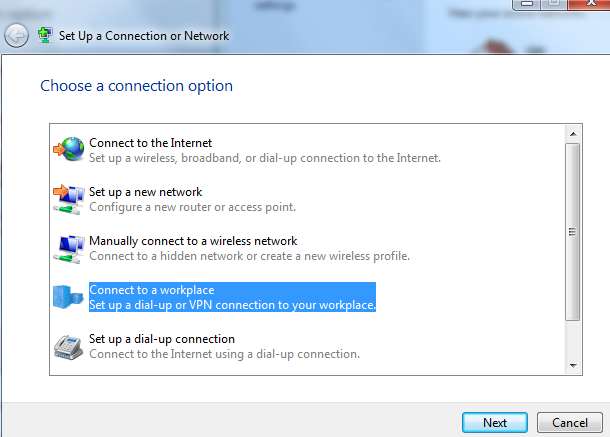
1. Cài đặt

**a. Windows server 2008**

Để sử dụng dịch vụ truy cập từ xa trong windows server, thông thường ta sử dụng mạng riêng ảo VPN (Virtual Private Networks). Dịch vụ VPN được cung cấp thông qua dịch vụ truy nhập từ xa và định tuyến RRAS (Routing and Remote Access Services). Trên máy chạy windows server, truy cập vào “Server Manager” → “Add Roles” → tích chọn “Network Policy and Access Services” → tích vào ‘Routing and Remote Access Services” và cài đặt

Tiếp theo, người quản trị cần cài đặt cấu hình cho máy chủ RRAS. Trên máy chạy windows server vào “Server Manager” → “Routing and Remote Access” → click chuột phải chọn “Configure and Enable Routing and Remote Access” → “Remote access (dial-up or VPN) → tích chọn VPN → Lựa chọn card mạng có kết nối với mạng công cộng như mạng Internet để VPN clients có thể truy cập→ Chọn khoảng cấp địa chỉ IP hoặc để tự động → Tích vào lựa chọn không sử dụng RADIUS server và hoàn thành phần cài đặt. Sau đó, máy chủ sẽ khởi động lại dịch vụ RRAS.



Để người dùng truy cập được máy chủ thông qua VPN, người dùng cần vào “Network and Sharing Center” → “Set up a new connection or network” → “Connect to a workplace” → Use my Internet connection (VPN) → Điền địa chỉ IP cho dịch vụ VPN và tên điểm đến → Nhập user name và password mà người quản trị đã cung cấp và kết nối.

**b) Ubuntu server**

Để sử dụng dịch vụ truy cập từ xa, ta sẽ sử dụng phiên bản miễn phí của dịch vụ truy nhập bảo mật SSH (Secure Shell) là OpenSSH. Trên máy chủ Unbutu, người quản trị sử dụng câu lệnh để cài đặt

sudo apt-get install openssh-server

Sau khi cài đặt, khởi động lại bằng câu lệnh:

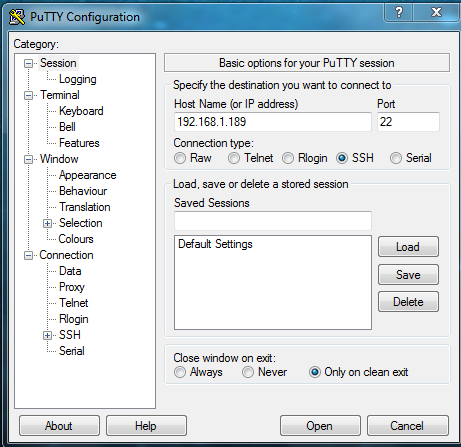
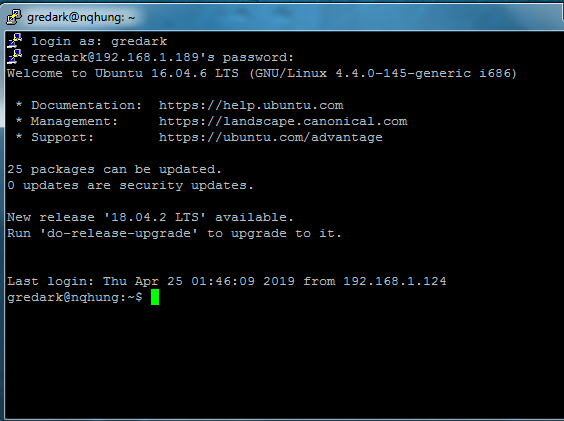
sudo service ssh restart

Để người dùng truy cập từ xa vào máy chủ Ubuntu server, trên máy chạy linux, người dùng sử dụng câu lệnh

sudo apt-get install openssh-client

Sau đó sử dụng câu lệnh sau để kết nối:

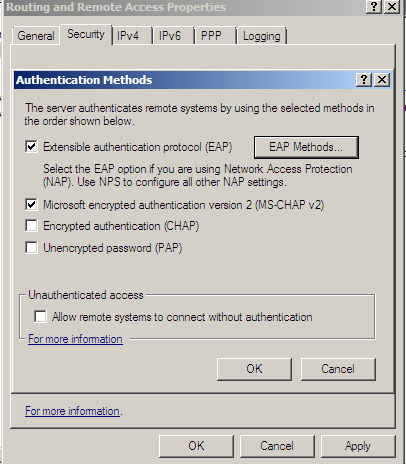
ssh tên\_người\_dùng@máy\_chủ\_SSH

Còn trên máy chạy windows, ta sử dụng phần mềm PuTTY. Người dùng điền địa chỉ IP của máy chủ Ubuntu, cổng mặc định sẽ là 22 và ấn Open. Màn hình đăng nhập hiện lên để người dùng nhập tên người dùng và mật khẩu của tài khoản trên máy chủ Ubuntu.

**2. Quản trị**

**a) Windows Server 2008**

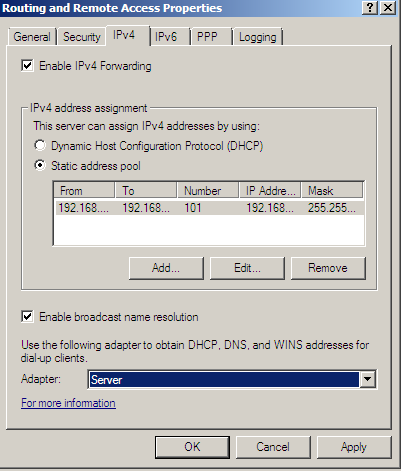
Trên máy chủ đã cài dịch vụ RRAS, vào “Server Manager” → click chuột phải trong phần “Routing and Remote Acces” chọn “Properties”.

-Security: người quản trị có thể chọn phương thức xác thực cho kết nối VPN. Windows Server 2008 cung cấp 4 phương thức xác nhận:

+Extensible authentication protocol (EAP): cho phép người dùng xác thực qua smart card hoặc digital certificates.

+Microsoft encryted authentication version 2 ( MS-CHAP v2): phương thức này cung cấp xác thực tương hỗ và cho phép mã hóa cả dữ liệu xác thực và dữ liệu kết nối.

+Encryted authentication (CHAP): phương thức này mã hóa dữ liệu xác thực bằng MD5 hashing.

+Unencrypted password (PAP) : khi sử dụng phương thức này, dữ liệu xác minh sẽ không được mã hóa mà truyền thẳng qua mạng ở dạng bản rõ.

-IPv4: cho phép người quản trị chỉ rõ dải địa chỉ mà người dùng có thể được gán thông qua

+Dynamic Host Configuration Protocol (DHCP): sử dụng DHCP server để tự động gán địa chỉ cho người dùng

+Static address pool: gán một khoảng địa chỉ IP tĩnh mà người quản trị muốn gán cho người dùng

**b) Ubuntu server**

Trên máy chủ Ubuntu, thông tin cấu hình được lưu trong file /etc/ssh/sshd\_config. Để sửa đổi thông tin cấu hình, người quản trị sử dụng câu lệnh

sudo nano /etc/ssh/sshd\_config

Trong file cấu hình, người quản trị có thể thay đổi một số tham số tiêu biểu sau:

-Cổng mà SSH server sử dung: Port 20

-Hoạt động trên địa chỉ: ListenAddress 192.168.1.189

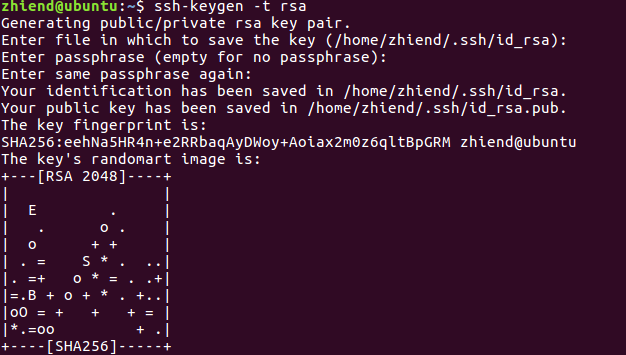
-Áp dụng xác thực RSA: RSAAuthentication yes

-Áp dụng xác thực mã khóa công khai: PubkeyAuthentication yes

-Hiện thông báo trong file issue.net khi đăng nhập: Banner /etc/issue.net

-Cho phép người dùng sử dụng SSH: AllowUser tên\_người\_dùng

-Cấm người dùng sử dụng SSH: DenyUsers tên\_người\_dùng

SSH server có cung cấp SSH key cho phép xác thực giữa hai host mà không cần mật khẩu giúp việc đăng nhập dễ dàng và an toàn vào máy chủ Ubuntu. SSH key bao gồm khóa công khai và khóa bí mật. Để tạo 2 khóa này, người dùng sử dụng câu lệnh:

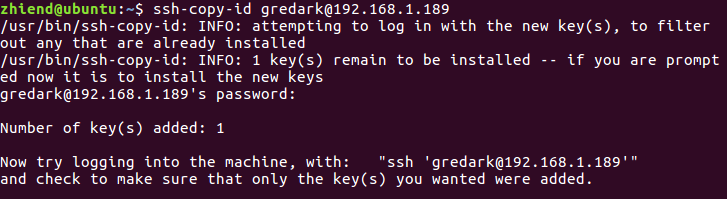
ssh-keygen –t rsa

Khóa công khai được lưu tại ~/.ssh/id\_rsa.pub

còn khóa bí mật lưu tại ~/.ssh/id\_rsa.

Để sử dụng khóa công khai trong quá trình xác thực, người dùng cần chép khóa vào máy chủ qua câu lệnh

ssh-copy-id tên\_người\_dùng@máy\_chủ\_ssh



Cuối cùng, kiểm tra quyền truy cập file chứa khóa xác thực authorized\_key, chỉ có người dùng đã được xác thực mới có quyền đọc hoặc ghi. Nếu quyền truy nhập vào file chứa khóa xác thực chưa phù hợp thì phải cập nhật lại theo câu lệnh sau:

chmod 600 .ssh/authorized\_keys